==========

H I P A A L E R T Volume 2, Number 13 October 29, 2001

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <

==========

HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total nearly 15,000.

Do you have interested associates? They can subscribe free at: http://www.hipaadvisory.com/alert/

IF YOU LIKE HIPAALERT, YOU'LL LOVE HIPAADVISORY.COM! -- Phoenix' comprehensive "HIPAA hub of the Internet" per Modern Healthcare. Visit: http://www.hipaadvisory.com

==========

T H I S I S S U E

==========

1 / F R O M T H E E D I T O R S:

Thanks to all who contributed to the Fall HIPAA Compliance Survey! Conducted in early October, this was the 7th in our series of quarterly Online HIPAA surveys, and the second to be co-sponsored by HIMSS.

The Fall Survey served as a half-way marker in the two-year HIPAA Transactions Rule compliance period (deadline: October 16, 2002). Will the industry be ready to accept and receive HIPAA transactions 12 months from now? In July, we reported several positive indicators; today, we are able to do the same -- PLUS a number of danger signals, as you will see.

Not surprisingly, much in our HIPAAnews section focuses on healthcare

security issues and HIPAA-related fallout from the national security crisis. Finally, in light of these new healthcare security concerns, our HIPAAdvisors answer a frequent question: "How much security is enough?"

Bruce Hall
Web Director / Editor

D'Arcy Guerin Gue
Publisher

==========

*** Bush Signs Anti-Terrorism Surveillance Bill into Law ***

President Bush signed into law on Friday an anti-terrorism package, called the Patriot Act, giving law enforcement vast new powers despite warnings from human rights and privacy advocates that the legislation goes too far. The final legislation does include a few changes: most notably, a sunset on the electronic surveillance provisions, and an amendment providing judicial oversight of law enforcement's use of the FBI's Carnivore system. However, it retains provisions vastly expanding government investigative authority, especially with respect to the Internet. Read more, including the ACLU's and EPIC's reactions:
http://www.hipaadvisory.com/news/2001/1026patriot.htm

*** Governors Renew Efforts to Support HIPAA Delay ***

On October 4, the National Governors Association (NGA) sent a letter to key House and Senate members. The letter included a list of policy options for Congress to consider in developing its final economic stimulus plan. The NGA updated its recommendations in a second letter sent Thursday, noting that if the House economic stimulus bill is enacted, it would further reduce state revenues by at least $5 billion annually. Without any changes in HIPAA or new federal funding for HIPAA implementation in state-administered programs, states will have to divert funds to comply. According to the NGA, "This means that significantly less state funds will be available for education, critical state services, capital investment, infrastructure improvement, and additional efforts to respond to bioterrorism and other threats to homeland security." Full Story:
http://www.hipaadvisory.com/news/2001/1005nga.htm

*** Shoring Up Internal System Security Helps Protect Against

External Threats ***

As users gear up to protect systems against external cyberterrorism threats, they also will have to consider locking down internal security by better managing the identity of their end-users. This point was recently underscored by industry members who were in New York to explore Gartner's findings that companies are indeed ramping up enterprise identity management initiatives because of government compliance, cost savings, and the benefits of easing administrative burdens. For Louisville-KY based Baptist Healthcare System's statewide hospital network, HIPAA proved the biggest justification for the organization's heightened internal security. Running a fine-tooth comb over possible internal threats allowed the organization to patch up or eliminate dormant rogue accounts, close exposed backdoors, and provide a much clearer picture of system vulnerabilities and multiple access points. Read more: http://www.hipaadvisory.com/news/index.htm#1022iw

*** New Report Urges HIPAA Support of Racial/Ethnic Health Data Sharing ***

A new report from The Commonwealth Fund finds wide gaps between the goals of federal initiatives to eliminate racial and ethnic disparities in health care and how federal health agencies are collecting the data needed to achieve these goals. The report, "Racial, Ethnic, and Primary Language Data Collection in the Health Care System: An Assessment of Federal Policies and Practices," calls for DHHS to take a leadership role in meeting the challenges of collecting and reporting health data that include information on race, ethnicity, and primary language. Full Story: http://www.hipaadvisory.com/news/2001/1022tcf.htm

*** Hospital Taps Biometrics for Single Sign-on ***

St. Vincent Hospital and Health Services in Indianapolis has rolled out a biometric authentication pilot project that combines the practicality of single sign-on workstations with biometric authentication devices for roaming enterprise users, reports ComputerWorld. "Biometrics has become synonymous with single sign-on," said Bruce Peck, information security manager at St. Vincent. "We saw this as a way to raise the bar for security across the board." The hospital is showing itself to be a robust proving ground for the combination of the two capabilities. And officials at both the hospital and the software vendors said they're confident that if it can work there, it can work at any company. "The key thing is to get users on and off the workstations quickly. If it slows them down, it impacts patient care," said Peck. Read more: http://www.hipaadvisory.com/news/index.htm#1029cw

==========
3 / H I P A A survey: Fall 2001 Survey Results

*** One Year to Transactions Deadline - Are We on Target? ***

by D'Arcy Guerin Gue, Exec Vice President, Phoenix Health Systems

As the final Fall 2001 HIPAA Survey results arrived in mid-October, The 1 year anniversary of the HIPAA Transactions Rule's effective date passed - giving the industry exactly 12 months to meet the compliance deadline. Will it be ready?

Over half of all survey participants, across all segments of the healthcare industry, reported that their organizations are actively working on HIPAA assessments and project planning. Many have begun implementations, primarily on Transactions and Privacy requirements. However, there are other indicators that industry-wide readiness for the October 16, 2002 Transactions deadline is questionable - even unlikely. 11% of all participants stated that their organizations are planning to "do nothing and see what happens" - certainly a precarious position. Moreover, though 45% of hospital respondents have either completed their HIPAA assessments or expect to by January 2002, their activity reflects less momentum than indicated in our July survey. At that time, nearly 80% of hospital respondents projected that their assessments would be complete by yearend.

Another trend that does not bode well for on-time Transactions compliance is that 16% of vendors reportedly will not be ready to transmit or accept all transactions by the deadline. Neither, apparently, will 7% of payers - although it is possible that those reporting represented small health plans, which have until 2003 to comply.

Finally, the most frequently cited roadblock to compliance reported by providers was "not enough time." While it can be argued that, for the large numbers just starting compliance initiatives, this is an issue they created, the probability remains that many who have claimed "not enough time" are forecasting correctly.

Other Indicated Trends:

> Reportedly, most provider organizations are engaged in compliance activities. However, the data suggests that the smaller the organization the slower the progress, and the greater the concerns about budgets and time constraints.

> Given the costs of comprehensive assessment and implementation, reported budgets for as many as half of hospital providers appear insufficient.

> According to over 80% of vendor representatives, their product quality will be improved as a result of HIPAA-related changes and updates.

> Half of payer respondents indicated that their organizations are addressing remediation on their own, without coordinating with their clients.

> One fifth of all participants noted that their management is providing little or no compliance support.

HIPAA AND THE NATIONAL SECURITY CRISIS

One final trend that deserves special attention relates to the impact of the current national security crisis on HIPAA-required security. Surprisingly, only 8% of the entire participant group - and even fewer provider representatives - reported that their organizations' attention to security has been affected "quite a lot, or greatly." The overwhelming majority recorded little or no change in their security focus.

THE SURVEY

During the first ten days of October, Phoenix Health Systems and HIMSS conducted the Fall 2001 Healthcare Industry HIPAA Compliance Survey - the seventh quarterly survey in an ongoing series. Following E-mail appeals to HIMSS 12,000+ members and to Phoenix' 15,000 HIPAAlert newsletter subscribers, 519 healthcare industry representatives responded. The online survey was completed anonymously via Phoenix' website HIPAAdvisory.com.

Because of concerns about smaller providers' unique issues, the Fall survey broke out hospitals with less than 100 beds into a separate provider category. Additionally, large physician groups with 30 or more physicians were included with "other providers," and practices with less than 30 physicians were separated into their own category. Respondents from provider organizations accounted for 66% (343) of participants. The breakout of participants follows:

> Hospitals - 50%
  > 400+ beds: 18%
  > 100-400 beds: 25%

  > Less than 100 beds: 7%
  > Other providers, including physician practices of 30+ physicians: 10%
  > Small physician practices of less than 30 physicians: 7%
> Payers - 20%
> Vendors - 12%
> Clearinghouses - 2%

Compliance officers and IT management each represented about 25% of total respondents; 20% were department managers, and 15% senior managers. About 80% of all respondents reported that they have official HIPAA roles within their organizations.

HIPAA AWARENESS AND MANAGEMENT SUPPORT

Nearly 75% of their organization's department heads and senior management were judged by respondents as having moderate to high knowledge of HIPAA and its implications. However, overall levels of awareness remained essentially unchanged from our last three survey results. The level of reported management awareness may seem high, but the fact remains that 25% of managers were judged as still having little or no awareness of HIPAA - despite the fact that two final HIPAA regulations are now in effect.

About 20% of all participants claimed that their management is providing little or no compliance support; and 46% felt that HIPAA was receiving moderately high or high support. Results from provider representatives were nearly identical. Given the widely accepted tenet that management buy-in is critical to successful HIPAA implementation, we must conclude that implementation initiatives - probably the most expensive aspect of compliance - may encounter roadblocks or delays in these organizations.

IMPACT OF NATIONAL SECURITY CRISIS

When asked how the current national security crisis has affected their organizations' sense of urgency regarding HIPAA security implementation, 67% of all participants reported either "not at all" or "a little." Only 6% of provider respondents and 8% of all respondents felt that their organizations' attention to security was affected "quite a lot or greatly". This outcome was surprising and of some concern to survey analysts, in light of the strong relationship between the national security environment and healthcare services, and in view of recent strong directives from the AHA and the AMA to upgrade enterprise security.

FOCUS OF ENTERPRISE HIPAA EFFORTS

Implementation Approach

Participants were asked to describe their organizations' compliance approach: "basic compliance", "incorporate HIPAA in strategic plans to achieve HIPAA's benefits", "best practices approach to exceed HIPAA requirements", "undecided", or "do nothing and see what happens".

Positive Approaches

More respondents reported using a "strategic" approach than any other- between 40-50% of each group. The exceptions were <100 bed hospitals (32%) and hospitals with 100-400 beds (37%). 30% of vendors and 40% of clearinghouse respondents reported using a "best practices" approach, but significantly fewer members of other industry segments are applying best practices (a range of 12-18%). More respondents from payer organizations (35%) and <100 bed hospitals (also 35%) reported using a "basic compliance" approach than any other group. A range of 18-28% of the remaining industry segments reported doing basic compliance, excluding clearinghouses - none of which were using a basic approach.

"Do-Nothing" Approach

A relatively small but significant percentage of participants (11%) Said that their organizations would "do nothing and see what happens." That they selected this answer rather than "undecided" suggests that the inaction is a deliberate choice rather than a result of ignorance or confusion. More participants from hospitals with 100-400 beds (15%) and from small physician practices (also 15%) projected that they would "do nothing" than any other groups. About 7% of respondents from 400+ bed hospitals and payers, and 11% of all remaining groups also chose this answer. The single exclusion was clearinghouse representatives, none of whom plan non-compliance. An average of 3% of all respondents were undecided.

AREAS OF CURRENT COMPLIANCE ACTIVITY

AWARENESS - Between 2/3 and 3/4 of all those surveyed noted that they were currently engaged in awareness efforts - generally in all regulatory areas of HIPAA.

ASSESSMENTS - A range of 1/2 to 3/4 of all participants reported that they are currently conducting HIPAA assessments.

> Hospitals - Hospitals with over 400 beds appear to lead the hospital industry in assessment activity: 75% were reported to be conducting assessments related to Transactions and Privacy, and 2/3 in Security. About 1/3 are including Identifiers in their assessments. 2/3 of hospitals in the 100-400 bed category reportedly are doing assessments addressing Transactions, Privacy and Security. Half of <100 bed hospitals were reported to be focusing on Transactions, with 2/3 addressing Privacy and Security issues.

> Other Providers - As reflected in our Summer Survey results, other providers including physician practices lag behind hospitals in performing impact assessments. Nevertheless, it appears that their assessment efforts have stepped up: about half of this group, including respondents from large and small physician practices, said they are working on enterprise HIPAA assessments.

> Payers, Vendors and Clearinghouses - Just under 3/4 of payer, vendor and clearinghouse respondents stated their organizations are conducting impact assessments - primarily in the areas of Privacy, Security and Transactions.

PROJECT PLANNING AND IMPLEMENTATION

A range of 50% to 75% of all participants reported that they are conducting HIPAA project planning; between 25% and 50% of all groups are working on implementation, primarily in Transactions and Privacy.

Hospitals - Among hospitals with over 400 beds, participants Reported that 2/3 are preparing Transactions, Privacy and Security project plans; 1/3 are already working on implementation. Half of respondents from <400 bed hospitals and 100-400 bed hospitals are doing Transactions and Privacy project plans, with less emphasis on Security; and about 25% are working on implementations in the same areas. For all hospital groups, these results represent essentially no change from the Summer Survey results.

> Other Providers - About 50% of other provider respondents and 30% of small practices indicated that they are doing project planning. Slightly less than 20% of other providers have started work on implementation.

> Payers, Vendors and Clearinghouses - A range of 2/3 to 3/4 of respondents from payers, vendors and clearinghouses reported doing Transactions and Privacy project plans, with 50% also planning Security. This represents almost no change from the Summer Survey responses in July. Between 1/3 and 1/2 of these groups indicated they are implementing Privacy and Transactions, with 25% including Security.

USE OF OUTSIDE CONSULTANTS

Like our July survey, more payer participants (66%) said they are engaging consultants for HIPAA compliance support than any other industry group. Just over 55% of 400+ bed hospitals, 42% of 100-400 bed hospitals and 38% of <100 bed hospitals are reportedly using consultants. Not surprisingly, considering the high cost of consultant support, only 30% of other providers, and 18% of small providers answered yes to this question. Of those using consultants, respondents indicated that this outside support was needed primarily for assessment and planning. Only 33% of payers and 5% to 10% of the various hospital segments using consultants expect to include consultants in implementation efforts.

PROVIDER BUDGETS

Provider respondents were asked how much their organizations are spending on HIPAA in 2001, and have budgeted for 2002. A large percentage of respondents (28% for 2001, 32% for 2002) reported not having these answers. The following excludes their responses:

2001 HIPAA Spending:

> Spending of all providers: 58% - less than $100K; 23% - $100K-$300K; 12% - $300K-$600K; 2% - $600K - 1 million; 5% - over $1 million

> In hospitals of more than 400 beds: 35% - less than $100K; 34% - $100K-$300K; 14% - $300K-$600K; 7% - $600K - 1 million; 10% - over $1 million

> In hospitals of 100-400 beds: 60% - less than $100K; 25% - $100K-$300K; 13% - $300K-$600K; 1% - $600K-1 million; 1% - over $1 million

> In <100 bed hospitals: 70% - less than $100K; 18% - $100K-$300K; 12% - $300K-$600K; 0% - $600K - 1 million; 0% - over $1 million

> By other providers, incl. large practices: 54% - less than $100K; 11% -$100K-$300K; 12% - $300K-$600K; 4% - $600K - 1 million; 18% - over $1 million

> Small physician practices: 100% - less than $100K.

2001 Spending: 400+ Bed Hospitals

2002 HIPAA Budgets:

> Budgets for all providers: 35% - less than $100K; 28% - $100K-$300K; 15% - $300K-$600K; 11% - $600K - 1 million; 11% - over $1 million

> In hospitals of 400+ beds: 9% - less than $100K; 32% - $100K-$300K; 19% -$300K-$600K; 15% - $600K - 1 million; 25 - over $1 million

> In hospitals of 100-400 beds: 28% - less than $100K; 40% - $100K-$300K; 18% - $300K-$600K; 13% $600K-1 million; 1% - over $1 million

> In <100 bed hospitals: 71% - less than $100K; 14% - $100K-$300K; 0% - $300K-$600K; 7% - $600K - 1 million; 7% - over $1 million.

> By other providers, incl. large practices: 54% - less than $100K; 11% - $100K-$300K; 12% - $300K-$600K; 4% - $600K - 1 million; 18% - over $1
million

> Small physician practices: 100% - less than $100K.

PROVIDERS - HIPAA ASSESSMENT COMPLETION

About 15% of all provider-based respondents reported that they have completed their HIPAA impact/gap assessments. 31% expect to be done in less than 3 months, 30% in 3 to 6 months, 10% in 7 to 12 months, and 2% after 12 months - later than the Transactions deadline. 10% did not know when their organizations' assessments were likely to be done.

Hospitals with over 400 beds appear farthest ahead: 25% of their representatives stated that assessments have been completed and another 26% expect to be done by yearend. Another 32% anticipated being finished within 3 to 6 months, and 12% in 7 to 12 months.

About 15% of 100 - 400 bed hospital representatives, <100 bed hospitals, and other providers have completed HIPAA assessments. 42% of 100-400 bed
hospital respondents expected to be completed in 3 months or less, 30% within 4 to 6 months, 6% in 7 to 12 months, and 3% after the deadline. 24% of <100 bed hospitals reportedly will complete assessments within 3 months, 18% in 4 to 6 months, and 15% within 7 to 12 months. 32% of other provider respondents, including large physician practices, anticipated completing assessments within 3 months, 32% in 4 to 6 months, 4% in 7 to 12 months, and 4% after the October 2002 deadline. Just 6% of small physician groups have conducted assessments; 12% expect

to be done in 3 months or less, 32% in 4 to 6 months, 21% in 7 to 12 months, and the remaining 6% after 12 months.

E-HEALTH AND HIPAA COMPLIANCE

Just over 50% of all provider respondents agreed that their organizations would need to be HIPAA-compliant in order to execute their E-health strategies. Considering the expense of E-health initiatives, it is not surprising that E-health strategies were reported most often by representatives of 400+ bed hospitals (59%) and 100-400 bed hospitals (53%).

COORDINATION EFFORTS WITHIN INDUSTRY

About 60% of all provider respondents noted that their organizations were actively coordinating compliance with vendors; about 40% said they were working with payers.

ROADBLOCKS TO COMPLIANCE

Providers were asked to rank-order several factors as impediments to their organizations' achieving HIPAA compliance: "Not enough time" was ranked as the greatest roadblock by more respondents (94) than any other factor. "Interpretation of the regulations" ranked #1 second most often (81 people); "budget constraints" was ranked #1 third most frequently (by 75 participants). A crosscheck of all items ranked #1 or #2 reaffirmed this result. Compared to other provider participants, those from <100 bed hospitals were most concerned about time (41%) and budget constraints (35%). 25% of all other groups ranked time constraints and budgets highest.

Ranking of Roadblocks by Provider Group

> All Hospitals: #1: not enough time, #2: budget constraints, #3: interpretation of regs

> Other Providers, including large physician groups: #1: budget constraints, #2: interpretation of regs, #3: not enough time

> Small Physician Practices: #1: interpretation of regs, #2: budget

constraints, #3: not enough time

READINESS TO DO HIPAA-COMPLIANT BUSINESS

The survey questioned participants from payers, clearinghouses and vendors concerning their organizations' progress in HIPAA remediation efforts. They were asked if they had begun coordinating compliance with their clients, and when they would be ready to use HIPAA transactions.

> Payers: Of the 106 payer respondents, about 50% said they have begun coordinating remediation with their clients - the other 50% are going it alone. This result is essentially identical to answers in the Summer Survey. About 10% said they are ready now to accept/transmit all HIPAA transactions. Another 15% expect to be ready within 3 months, 30% in 4 to 6 months, 38% in 7 to12 months, and 7% after the October 2002 Transactions compliance deadline.

> Clearinghouses: The sample of clearinghouse representatives was small -10 participants. 80% reported that they have begun coordinating remediation with clients. One person (10%) stated his organization was ready now to accept / transmit all HIPAA transactions, 30% will be ready in 4 to 6 months, and the remaining 60% in 7 to 12 months. All clearinghouse participants confirmed that they would be able to transmit and accept HIPAA transactions by the compliance deadline.

> Vendors: About 75% of vendor representatives said that they are coordinating remediation with clients. Slightly fewer than 15% said that their organizations have completed Transactions-related remediation or product development. Another 12% expect to be finished within 3 months, 28% in 4 to 6 months, 30% in 7 to12 months, and 16% do not expect to meet the compliance deadline next October.

Product Quality: Vendor representatives also were asked if they expected that the HIPAA-related product changes their firms were making would improve their product(s). Over 80% said they believed product quality would be higher.

To review these results, with charts and graphs, and to compare results with our previous surveys, go to http://www.hipaadvisory.com.

==========

Every quarter, we ask our survey participants for comments and every quarter, we get them. Here are the most thought-provoking:

COMPLIANCE COSTS

"While virtually no one can or does argue the merits of HIPAA, we are concerned with the deadlines, which may mean re-investing in systems that have not been fully amortized...it would have made more sense to require compliance over the horizon of system obsolescence and replacementwith a final deadline out at five to seven years. . . ." CIO, 100-400 bed hospital

"Our HIPAA compliance efforts are competing against many other strategic initiatives for resources, and it is not easy to obtain the people and money this project requires." Department Manager, 100-400 bed hospital

"I feel the biggest restraints are time & money. The regulations are easy enough to understand after you read them three or four times. There is a lot of work involved and coordinating with the vendors and payors is difficult." Other, 100-400 bed hospital

"Increased costs in economic slow down have us thinking of closing. HIPAA costs too much to start with a long term ROI. A delay or better yet, huge scale back is the only way I see to keep us little guys in the business." CIO/Payer

"There are few budget items discreetly identified as 'HIPAA.' However, there are many operations and capital initiatives that will include HIPAA objectives but the primary label will be specific projects oriented to the "best practices" concept." Senior Management, >100 bed hospital

DELAYS IN FINAL REGULATIONS

"Delays in finalization of regulations (i.e. Security) are causing a tremendous amount of difficulties in moving forward with HIPAA compliance. Funding is difficult to obtain when something is 'pending' vs. final." Other, Other Provider

"We feel strongly that HIPAA does need to move forward and not be delayed. . . . There are many benefits, especially in the transactions and code sets. . . . It's time for the health care industry to move forward, not backwards." Compliance/Security officer, Clearinghouse

"We will be ready to support our clients by October 2002 and urge HHS to not delay the TCS rules. We believe that delaying the rules would

not result in anything except a delay and at the end of that time, the same entities would still not be ready." Senior Management, Vendor

"Having security regulations final by December 2001 will be very helpful." Compliance/Security officer, 400+ bed hospital

"The longer groups try to delay the harder it is to get buy-in and dollars needed to implement the regs. The stalling needs to stop, or we will have no choice but to scramble late in the game." Other, Other Provider

CULTURAL PROBLEMS IMPLEMENTING HIPAA

"While our "management team" is aware of HIPAA and has had an "official" overview briefing, they do not seem committed to doing anything that will require spending money to comply. This is a source of real frustration for me, as I am the HIPAA Coordinator...." Compliance Coordinator, Other Provider

"The task of changing our product to support HIPAA compliance is being made somewhat difficult because our customers, mostly small to medium private practices, are not taking HIPAA as seriously as they should, nor are they taking on the responsibility that they should." Compliance/Security Officer, Vendor

"Our esteemed HIPAA Compliance officer gave us little direction except the message of "Do Something!" I have decided to take action within my department (Lab) and hope the rest of the hospital can find their own way." Department Manager,Other Provider

"As an InfoSec Director (security officer) it's good to finally see forward momentum on this project. I have excellent executive support. I am very concerned about vendor compliance." Compliance/Security Officer, 400+ bed hospital

"We are a state mental health organization with several state run hospitals, contracted private hospitals, and over 2000 county providers. The county providers will be the hardest hit by transactions and codes. The department has yet to pick, or seriously discuss, a strategy for bringing the counties into compliance." Analyst, Payer

"Starting the fire engine, gathering the firemen and finding which direction to go takes longer than getting to and putting out the fire." Compliance/Security Officer, 400+ bed hospital

==========
==========

5 / H I P A A d v i s o r: How Much Security is Enough?

Protecting the Safety of Individually Identifiable Health Information
by Steve Fox, Esq., and Rachel Wilson, Esq., Pepper Hamilton LLP

QUESTION: The Security Regulation requires covered entities to safeguard the integrity, confidentiality, and availability of individually identifiable health information ("IIHI"). But how can a covered entity be expected to guard against any and all conceivable threats to this information? Does HHS really expect us to protect IIHI from the vast universe of potential security breaches regardless of the likelihood of any one type of occurrence?

ANSWER: Covered entities are not expected to guarantee the safety of IIHI against any and all threats. Compliance with the Security Regulation requires covered entities to implement and maintain reasonable safeguards to protect against reasonably anticipated threats. However, an entity's chosen security initiative may be called into question in the event that the entity is the subject of a compliance audit.

The Security Regulation requires covered entities to make an assessment of the vulnerabilities and potential risks to the IIHI in their possession and then develop, implement, and maintain appropriate security measures to safeguard the integrity, confidentiality, and availability of that data. These measures must be documented in a security plan and kept current.

The Security Regulation is scalable and technology neutral. The resources and vulnerabilities of any particular covered entity will determine the scope and nature of the security that is implemented. For example, the Regulation's authentication requirement can be met through the utilization of a six-character password or by using biometrics technology. The choice to implement one authentication tool over the other will be based in large part on two factors. First, the likelihood that a security breach will occur - the vulnerability of the IIHI in the entity's possession. Second, an assessment of the damage that could result from such a breach in security - the potential risk to the IIHI in the covered entity's possession. Because entities may be called upon to defend their risk assessment and corresponding security implementation, it would be prudent to undergo periodic risk assessments in order to insure that the entity's security initiative represents a realistic, current, and comprehensive approach to protecting the IIHI in its possession and control.

The Security Regulation has not yet been released in final form, so it is possible that these requirements may be modified in the final

version. However, HHS officials have stated publicly that the basic philosophy underlying the final Security Regulation will remain unchanged and that the final regulation will be streamlined to avoid redundancies with other HIPAA rules, as well as to eliminate excessive micromanagement. Most commentators do not believe that major substantive changes to the proposed Security Regulation are likely because of the close interaction and interdependence of security and the final Privacy Rule.

To read past HIPAAdvisor articles, go to:
http://www.hipaadvisory.com/action/HIPAAdvisor.htm

Steve Fox, Esq., is a partner at the Washington, D.C., office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., an associate at Pepper Hamilton LLP. http://www.pepperlaw.com/

Disclaimer: This information is general in nature and should not be relied upon as legal advice.

==========
COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit http://www.hipaadvisory.com/alert/
ARCHIVES: http://www.hipaadvisory.com/alert/newsarchives.htm
==========

==========

FORWARD this posting to interested associates, who may subscribe free to HIPAAlert at: http://www.hipaadvisory.com/alert/
Subscribe to our free discussion list at:
http://www.hipaadvisory.com/live/ Get a weekly byte of HIPAA at:
http://www.hipaadvisory.com/notes/
Switch to HTML version or to text version at:
http://www.hipaadvisory.com/signup/change.cfm

FORWARD this posting to interested associates, who may subscribe free to HIPAAlert at:
http://www.hipaadvisory.com/alert/
Subscribe to our free discussion list at:
http://www.hipaadvisory.com/live/
Get a weekly byte of HIPAA at:
http://www.hipaadvisory.com/notes/
Switch to HTML version or to text version at:
http://www.hipaadvisory.com/signup/change.cfm

You are currently subscribed to hipaalert as:kmckinst@dmhhq.state.ca.us

To UNSUBSCRIBE, send a blank e-mail to:
leave-hipaalert-8507990O@lists.hipaalert.com
or just send an e-mail to:
lyris@lyris.dundee.net
and in the body of the message type:
unsubscribe hipaalert [your e-mail address]